

Cryptanalysis of a Simple Three-party Key Exchange Protocol

N.W. Lo¹, Kuo-Hui Yeh² and Meng-Chih Chiang³

Department of Information Management
National Taiwan University of Science and Technology
No.43, Sec.4, Keelung Rd., Taipei, Taiwan (R.O.C.)
nwlo@cs.ntust.edu.tw¹; [{D9409101²; m9709101³ }@mail.ntust.edu.tw](mailto:{D9409101@m9709101}@mail.ntust.edu.tw)

Abstract. Three-party authenticated key exchange (3PAKE) protocol plays an indispensable role in history of the secure communication areas in which two clients can agree a robust session key based on a human-memorable password. Current research community focuses on the issue of designing a simple 3PAKE (S-3PAKE) protocol which possesses both of robust system security and efficient computation complexity. In 2008, Chung and Ku [4] pointed out that Lu and Cao's S-3PAKE scheme [12] cannot resist three variants of the man-in-the-middle attack. The authors proposed a countermeasure to eliminate the identified weaknesses. Nevertheless, based on our security analysis, the S-3PAKE mechanism proposed by Chung and Ku is vulnerable to the undetectable on-line dictionary attack. In this paper, we review Chung and Ku's S-3PAKE protocol and analyze its robustness. For security enhancement, a modified S-3PAKE scheme is introduced to resist to the undetectable on-line dictionary attack

Keywords: 3PAKE, authentication, cryptanalysis, security, undetectable on-line dictionary attack.

1 Introduction

To achieve secure communication within a hostile network, 3PAKE mechanism is widely deployed on lots of remote user authentication system due to its simplicity and convenience of maintaining a human-memorable password at client side. In a normal 3PAKE protocol, each communication client shares an easy-to-remember password with a trusted server in advance. Once any two clients intend to establish a robust session key, both of them resort to the server and their shared passwords to authenticate each other. After that, only legitimate client can be authorized to derive the current session key.

Since Bellare and Merrit [1] first proposed a two-party encrypted key exchange protocol based on user passwords, many two-party password-based authenticated key exchange (2PAKE) protocols have been investigated. However, the 2PAKE protocols

are only suitable for client-server architecture [4]. This limitation inspires research community to extend 2PAKE protocols into 3PAKE schemes for three-party communication environment, i.e. client-client-server model. Meanwhile, the low-entropy of human-memorable password make 3PAKE protocols vulnerable to a so-called exhaustive dictionary attack while the rapidly development of semiconductor technology can greatly reduce the computation time of malicious password guessing and verification procedures than before. The dictionary attack is a series of challenge-response malicious procedures in which adversary can iteratively try-and-guess the secret password of victim communication party until discovering the correct one. In general, the dictionary attack can be classified into three types [5].

- Detectable on-line dictionary attack: an attacker attempts to utilize guessed password in an on-line transaction and verify the correctness of his/her guessed password via the responses from server. But a failure can be easily detected and logged at server side.
- Undetectable on-line dictionary attack: Similarly, an attacker tries to guess a password and verify it in an on-line transaction. However, a failed guess cannot be detected and logged by the server, as server is not able to distinguish an honest request from a malicious one.
- Off-line dictionary attack: an attacker guesses a password and verifies his/her guess off-line. No participation of server is required, so the number of guesses have no limitation.

In spite of many scholars [2-17] had focused on secure 3PAKE mechanism design, most of them suffer from variant malicious attacks and the dictionary attack. In 1995, Steiner et al. [15] developed an authentication protocol to improve the system efficiency of Bellovin and Merrit's mechanism by reducing the number of transmission rounds and cryptographic operation. Unfortunately, the authors in [5] and [10] had demonstrated that Steiner et al.'s scheme cannot resist against the undetectable on-line dictionary attack and off-line dictionary attack. To enhance its security, Lin et al. [10] adopted the public key cryptosystem technology to construct a remedy scheme. However, the computation cost of public key en/decryption is too high to be adopted in a 3PAKE protocol. Hence, Lee et al. [8] introduced two enhanced three-party encrypted key exchange protocols to achieve mutual authentication and provide perfect forward secrecy in which the public key cryptosystem is not required. Later, Wen et al. [17] utilized weil pairing concept to establish a 3PAKE protocol with formal proof model. Nevertheless, Nam et al. [13] showed that Wen et al.'s protocol is vulnerable to a man-in-the-middle attack, and interpreted their proposed attack in the context of the formal proof model.

Designing a 3PAKE protocol which possesses both of system security and computation efficiency is particularly a challenge due to the difficult tradeoff among security robustness, system performance and computation cost. In 2007, Lu and Cao [12] developed an S-3PAKE protocol to pursue the security requirements and the efficiency criteria. However, their protocol suffers from man-in-the-middle attacks and undetectable on-line dictionary attack [6 and 14]. Later, Chung and Ku [4] proposed a security enhanced S-3PAKE mechanism which is based on Lu and Cao's protocol. Nevertheless, Chung and Ku's protocol is not without its flaws. In this paper, we find that the S-3PAKE scheme proposed by Chung and Ku is insecure against the undetectable on-line dictionary attack in the presence of an active attacker. A remedy

mechanism is then introduced to eliminate the identified vulnerability.

The rest of this paper is organized as follows. Section 2 briefly reviews Chung and Ku's S-3PAKE protocol followed by its robustness analysis. Next, we introduce our proposed protocol in section 3 and the security analysis in section 4, respectively. Finally, the concluding remarks are summarized in Section 5.

2 Security analysis of Chung and Ku's S-3PAKE protocol

In this section, we briefly review Chung and Ku's S-3PAKE scheme and analyze its robustness, i.e. the resistance to undetectable on-line dictionary attack. Before that, we define some notations which will be utilized in this paper.

- A, B : the communication client.
- ID_A, ID_B : the identity of A and B , respectively.
- S : the trusted server.
- ID_S : the identity of S .
- (G, g, p) : a finite cyclic group G generated by an element g of prime order p .
- M, N : two elements in G .
- \parallel : bitwise concatenation.
- PW_1 : the password shared between A and S .
- PW_2 : the password shared between B and S .
- H, H' : two secure one-way hash functions.

2.1 Chung and Ku's S-3PAKE scheme

This section briefly introduce Chung and Ku's S-3PAKE method in which two clients A and B intend to establish a robust session key via a previously shared secret password. A trusted server S is assumed. The detailed procedures of the normal session are presented as follows (Figure 1).

1. $A \rightarrow B: ID_A \parallel X$

Client A generates a random number $x \in Z_p$ and calculates $X \leftarrow g^x \cdot M^{PW_1}$. Next, A sends $ID_A \parallel X$ to client B as a communication request.

2. $B \rightarrow S: ID_A \parallel X \parallel ID_B \parallel Y$

Similarly, B calculates $Y \leftarrow g^y \cdot N^{PW_2}$ where $y \in Z_p$ is a random number. Then, B sends $ID_A \parallel X \parallel ID_B \parallel Y$ to the trusted server S .

3. $S \rightarrow B: X' \parallel Y'$

Once receiving the message $ID_A \parallel X \parallel ID_B \parallel Y$, S first retrieves the corresponding passwords PW_1 and PW_2 and computers the following equations, where $z \in Z_p$ is a random number. Next, S issues the values X' and Y' to B .

$$g^y \leftarrow Y/N^{PW_2}, g^{yz} \leftarrow (g^y)^z, X' \leftarrow g^{yz} \cdot H(ID_A, ID_B, ID_S, g^x)^{PW_1}$$

$$g^x \leftarrow X/M^{PW_1}, g^{xz} \leftarrow (g^x)^z, Y' \leftarrow g^{xz} \cdot H(ID_B, ID_A, ID_S, g^x)^{PW_2}$$

4. $B \rightarrow A: X' || \alpha$

Upon getting the response X' and Y' , B utilizes the shared password PW_2 to retrieve $g^{yz} \leftarrow Y'/H(ID_B, ID_A, ID_S, g^y)^{PW_2}$. After that, B computes value $g^{xyz} \leftarrow (g^{xz})^y$ and a verification message $\alpha \leftarrow H(ID_A, ID_B, g^{xyz})$, and then sends $X' || \alpha$ to A .

5. $A \rightarrow B: \beta$

When A receives $X' || \alpha$, he/she first calculates $g^{yz} \leftarrow X'/H(ID_A, ID_B, ID_S, g^x)^{PW_1}$ and $g^{xyz} \leftarrow (g^{yz})^x$. A then checks whether received value α and computed value $H(ID_A, ID_B, g^{xyz})$ is the same or not. If these two values are different, A terminates the protocol. Otherwise, A is convinced that g^{xyz} is valid. Next, A calculates the current session key $SK_A \leftarrow H'(ID_A, ID_B, g^{xyz})$, and a verification message $\beta \leftarrow H(ID_B, ID_A, g^{xyz})$ which will be promptly forwarded to B . When B receives value β , he/she examines if $\beta = H(ID_B, ID_A, g^{yz})$ holds. If this process is verified successfully, B will also be convinced that g^{xyz} is valid. Otherwise, B terminates the protocol. Now B can compute its session key $SK_B \leftarrow H'(ID_A, ID_B, g^{xyz})$. Finally, both of A and B possess the same session key $SK_A = SK_B = H'(ID_A, ID_B, g^{xyz})$.

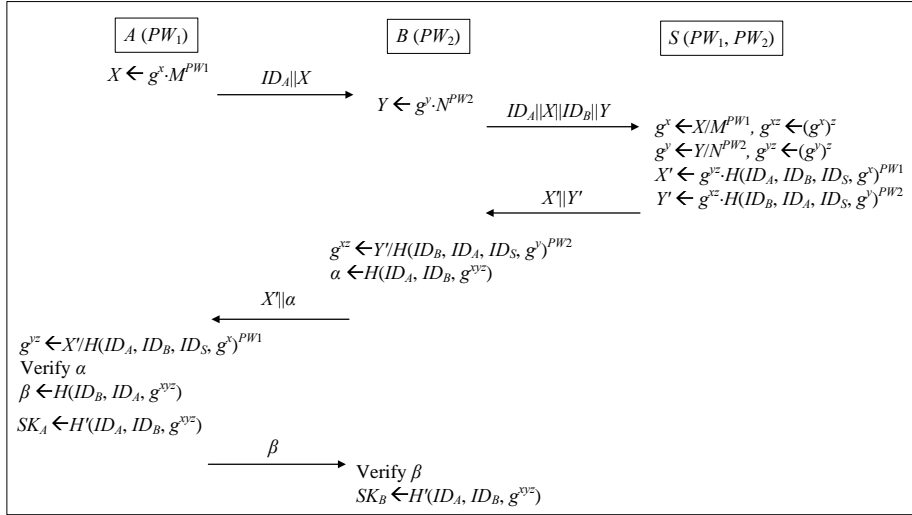


Figure 1: Chung and Ku's S-3PAKE protocol.

2.2 Undetectable on-line dictionary attacks

Chung and Ku's S-3PAKE protocol is not without its flaw. Based on our security analysis, we find that their scheme cannot resist to the undetectable on-line dictionary attack. The detailed procedures of this authentication flaw are shown as follows (Figure 2).

1. $A \rightarrow B: ID_A || X$

A operates normally as that in step 1 of Chung and Ku's S-3PAKE protocol.

2. $B \rightarrow S: ID_A || X || ID_B || Y$

Once B receives $ID_A || X$, he/she guesses a password PW' , and computes $g^{x'} \leftarrow X/M^{PW'}$ and $Y = g^{x'} \cdot N^{PW_2}$. Then, B sends $ID_A || X || ID_B || Y$ to S and abandons the current session communicated with A .

3. $S \rightarrow B: X' || Y'$

S operates normally as that in step 3 of Chung and Ku's S-3PAKE scheme.

$$g^y \leftarrow Y/N^{PW_2} = g^{x'} \cdot N^{PW_2}/N^{PW_2}, g^{x'z} \leftarrow (g^{x'})^z, X' \leftarrow g^{x'z} \cdot H(ID_A, ID_B, ID_S, g^x)^{PW_1}$$

$$g^x \leftarrow X/M^{PW_1} = g^x \cdot M^{PW_1}/M^{PW_1}, g^{xz} \leftarrow (g^x)^z, Y' \leftarrow g^{xz} \cdot H(ID_B, ID_A, ID_S, g^x)^{PW_2}$$

Once B receives the values X' and Y' , B utilize his/her own password PW_2 and guessed password PW' to retrieve the values g^{xz} and $g^{x'z}$.

$$g^{xz} \leftarrow Y'/H(ID_B, ID_A, ID_S, g^x)^{PW_2}, g^{x'z} \leftarrow X'/H(ID_A, ID_B, ID_S, g^{x'})^{PW'}$$

Next, B examines whether these two retrieved values g^{xz} and $g^{x'z}$ are identical or not. If this examination holds, B confirms that password PW' is correctly guessed.

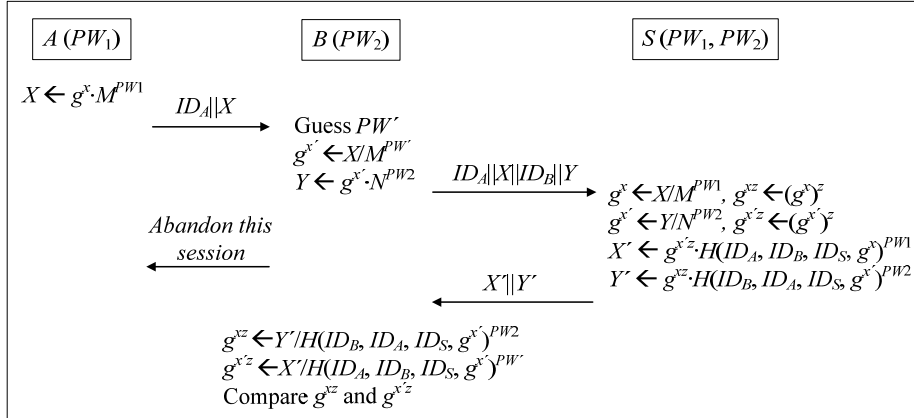


Figure 2: Undetectable on-line dictionary attack on Chung and Ku's protocol.

3 An enhanced S-3PAKE scheme

The undetectable on-line dictionary attack are a natural deficiency of all S-3PAKE mechanisms once it does not provide any verification process for the authenticity of transmitted request or response messages. Hence, in this section we develop a security enhanced S-3PAKE scheme, which is embedded with a message authentication process at server side, to more effectively withstand the undetectable on-line dictionary attack. The detailed procedures of our countermeasure are presented in Figure 3.

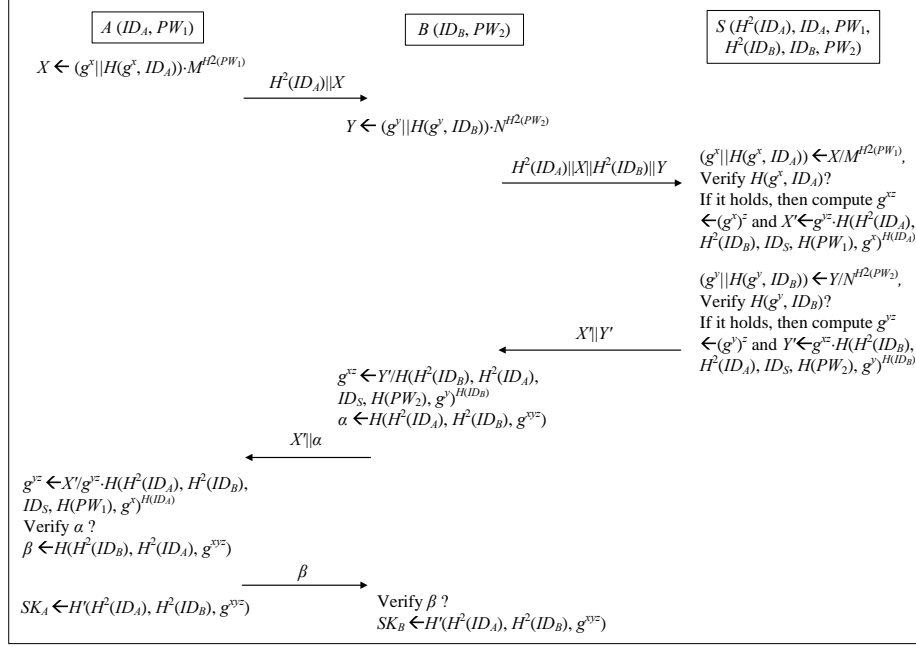


Figure 3: An enhanced S-3PAKE scheme.

1. $A \rightarrow B: H^2(ID_A) || X$

Client A first inputs its identity ID_A and password PW_1 . Next, A generates a random number $x \in Z_p$, and calculates $H^2(ID_A)$ and $X \leftarrow (g^x || H(g^x, ID_A)) \cdot M^{H^2(PW_1)}$. Next, A sends $H^2(ID_A) || X$ to client B as a communication request.

2. $B \rightarrow S: H^2(ID_A) || X || H^2(ID_B) || Y$

Similarly, B inputs its identity ID_B and password PW_2 , and calculates $H^2(ID_B)$ and $Y \leftarrow (g^y || H(g^y, ID_B)) \cdot N^{H^2(PW_2)}$ in which $y \in Z_p$ is a random number. B then sends $H^2(ID_A) || X || H^2(ID_B) || Y$ to the trusted server S .

3. $S \rightarrow B: X' || Y'$

Once receiving the message $H^2(ID_A) || X || H^2(ID_B) || Y$, S retrieves the corresponding shared information ID_A , PW_1 , ID_B and PW_2 based on the received values $H^2(ID_A)$ and $H^2(ID_B)$. S then performs the following computations, where $z \in Z_p$ is a random number. Next, S issues the values X' and Y' to B .

$$\begin{aligned}
 &(g^x || H(g^x, ID_A)) \leftarrow X / M^{H^2(PW_1)}, \text{ verify } H(g^x, ID_A)? \text{ If it holds, then} \\
 &g^{yz} \leftarrow (g^y)^z, X' \leftarrow g^{yz} \cdot H(H^2(ID_A), H^2(ID_B), ID_S, H(PW_1), g^{x \cdot H(ID_A)}) \\
 &(g^y || H(g^y, ID_B)) \leftarrow Y / N^{H^2(PW_2)}, \text{ verify } H(g^y, ID_B)? \text{ If it holds, then} \\
 &g^{xz} \leftarrow (g^x)^z, Y' \leftarrow g^{xz} \cdot H(H^2(ID_B), H^2(ID_A), ID_S, H(PW_2), g^{y \cdot H(ID_B)})
 \end{aligned}$$

4. $B \rightarrow A: X' || \alpha$

Upon getting the response X' and Y' , B utilizes its identity ID_B and password PW_2 to retrieve $g^{yz} \leftarrow Y'/H(H^2(ID_B), H^2(ID_A), ID_S, H(PW_2), g^y)^{H(ID_B)}$. After that, B computes value $g^{xyz} \leftarrow (g^{yz})^y$ and a verification message $\alpha \leftarrow H(H^2(ID_A), H^2(ID_B), g^{xyz})$, and then sends $X' || \alpha$ to A .

5. $A \rightarrow B: \beta$

When A receives $X' || \alpha$, he/she calculates $g^{yz} \leftarrow X'/H(H^2(ID_A), H^2(ID_B), ID_S, H(PW_1), g^x)^{H(ID_A)}$ and $g^{xyz} \leftarrow (g^{yz})^x$. A then checks whether received value α is identical to computed value $H(H^2(ID_A), H^2(ID_B), g^{xyz})$. If these two values are the same, A is convinced that g^{xyz} is valid. Otherwise, A terminates current protocol. Next, A calculates a session key $SK_A \leftarrow H(H^2(ID_A), H^2(ID_B), g^{xyz})$, and a verification message $\beta \leftarrow H(H^2(ID_B), H^2(ID_A), g^{xyz})$. Then, A sends β to B . When B receives β , he/she examines if $\beta = H(H^2(ID_B), H^2(ID_A), g^{xyz})$ holds. If this verification process is passed successfully, B will believe that g^{xyz} is valid. Otherwise, B terminates current protocol. B then computes a session key $SK_B \leftarrow H(H^2(ID_A), H^2(ID_B), g^{xyz})$. Finally, both of A and B possess the same session key $SK_A = SK_B = H(H^2(ID_A), H^2(ID_B), g^{xyz})$.

4 Security analysis

In this section, we only discuss the enhanced security, i.e. the resistance to undetectable on-line dictionary attack, of our proposed S-3PAKE protocol.

Claim: The enhanced S-3PAKE scheme can more effectively resist to the undetectable on-line dictionary attack in comparison with Chung and Ku's protocol.

As mentioned before, the undetectable on-line dictionary attack is a natural deficiency of all S-3PAKE mechanisms which does not provide the verification procedures for the authenticity of transmitted messages. Therefore, our enhanced protocol adopts a message verification process, i.e. $H(g^x, ID_A)$ and $H(g^y, ID_B)$, at server side to prevent this potential security weakness. In addition, as we simultaneously utilize two well-concealed secret values, i.e. user's identity and password, to protect client's transmitted information, an adversary must devote at least twice computation efforts to invoke an undetectable on-line dictionary attack on our protocol in comparison with that in Chung and Ku's protocol. This makes our protocol more secure. Furthermore, each transmission message in our protocol is protected by various secret values such as $ID_A, H(ID_A), PW_1, H(PW_1), ID_B, H(ID_B), PW_2, H(PW_2)$. This design can eliminate the correlation between transmitted values and greatly reduce the possibility of invoking an undetectable on-line dictionary attack on our enhanced protocol. On these grounds, we believe that the proposed S-3PAKE scheme can more effectively resist to the undetectable on-line dictionary attack than Chung and Ku's protocol.

5 Conclusion

In this paper, we have demonstrated that a recent S-3PAKE protocol proposed by

Chung and Ku is insecure against the undetectable on-line dictionary attack. To eliminate the identified authentication weakness, we develop a remedy mechanism to achieve security enhancement. By adopting two newly proposed design concepts, i.e. (1) message authentication mechanism at server side and (2) hash-chain value based protection design, our enhanced S-3PAKE scheme is more secure and convinced than Chung and Ku's protocol in terms of resistance to the undetectable on-line dictionary attack.

Acknowledgments The authors gratefully acknowledge the support from TWISC project sponsored by the National Science Council, Taiwan, under the Grants No NSC 98-2219-E-011-001. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

1. S.M. Bellare and M. Merritt, "Encrypted key exchange: password-based protocols secure against password guessing attacks," in *Proc. of 1992 IEEE Symposium on Research in Security and Privacy*, pp.72-84, 1992.
2. C.C. Chang and Y.F. Chang, "A novel three-party encrypted key exchange protocol," *Computer Standards and Interfaces*, vol.26, no.5, pp.471-476, 2004.
3. T.H. Chen, W.B. Lee and H.B. Chen, "A round- and computation- efficient three-party authenticated key exchange protocol," *Journal of Systems and Software*, vol.81, pp.1581-1590, 2008.
4. H.R. Chung and W.C. Ku, "Three weaknesses in a simple three-party key exchange protocol," *Information Science*, vol.178, no.1, pp.220-229, 2008.
5. Y. Ding and P. Horster, "Undetectable on-line password guessing attacks," *ACM Operating Systems Review*, vol.29, no.4, pp.77-86, 1995.
6. H. Guo, Z. Li, Y. Mu and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," *Computers and Security*, vol.27, no.1-2, pp.16-21, 2008.
7. L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone, "An efficient protocol for authenticated key agreement," *Designs, Codes and Cryptography*, vol.28, no.2, pp.119-134, 2003.
8. T.F. Lee, T. Hwang and C.L. Lin, "Enhanced three-party encrypted key exchange without server public keys," *Computers and Security*, vol.23, no.7, pp.571-577, 2004.
9. S.W. Lee, H.S. Kim and K.Y. Yoo, "Efficient verifier-based key agreement protocol for three parties without server's public key," *Applied Mathematics and Computation*, vol.167, no.2, pp.996-1003, 2005.
10. C.L. Lin, H.M. Sun and T. Hwang, "Three party-encrypted key exchange: attacks and a solution," *ACM Operating Systems Review*, vol.34, no.4, pp.12-20, 2000.
11. C.L. Lin, H.M. Sun, M. Steiner and T. Hwang, "Three-party encrypted key exchange without server public-keys," *IEEE Communication Letters*, vol.5, no.12, pp.497-499, 2001.
12. R.X. Lu and Z.F. Cao, "Simple three-party key exchange protocol," *Computers and Security*, vol.26, no.1, pp.94-97, 2007.
13. J. Nam, Y. Lee, S. Kim and D. Won, "Security weakness in a three-party pairing-based protocol for password authenticated key exchange," *Information Sciences*, vol.177, no.6, pp.1364-1375, 2007.
14. C.W. Phan Raphael, W.C. Yau and B.M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)," *Information Sciences*, vol.178, no.13, pp.2849-2856, 2008.
15. M. Steiner, G. Tsudik and M. Waidner, "Refinement and extension of encrypted key

- exchange,” *ACM Operating Systems Review*, vol.29, no.3, pp.22-30, 1995.
16. H.M. Sun, B.C. Chen and T. Hwang, “Secure key agreement protocols for three-party against guessing attacks,” *Journal of Systems and Software*, vol.75, pp.63-68, 2005.
 17. H.A. Wen, T.F. Lee and T. Hwang, “Provably secure three-party password-based authenticated key exchange protocol using Weil pairing,” *IEE Proceedings – Communications*, vol.152, no.2, pp.138-143, 2005.